

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY

Feedback

random bit and digital stream bit and public

Terms used: random bit digital stream bit public

Sort results by:

Save results to a Binder

Refine these results
Try this search inDisplay results: ☐ Open results in a new window

Results 1 - 20 of 786

Result page: 1 2 3 4 5 6 7 8 9 10 next >>

1 Xor-trees for efficient anonymous multicast and reception



Shlomi Dolev, Rafail Ostrobsky

May 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue

Publisher: ACM

Full text available: Pdf (296.45 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 66, Citation Count: 4

We examine the problem of efficient anonymous multicast and reception in general communication networks. We present algorithms that achieve anonymous communication, are protected against analysis, and require $O(1)$ amortized communication ...

Keywords: anonymous communication, anonymous multicast

2 Revealing skype traffic: when randomness plays with you



Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, Paolo Tofanelli

August 2007 SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures and protocols for computer communications

Publisher: ACM

Full text available: Pdf (911.54 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 52, Downloads (12 Months): 745, Citation Count: 0

Skype is a very popular VoIP software which has recently attracted the attention of the research community and network operators. Following a closed source and proprietary design, Skype protocols algorithms are unknown. Moreover, strong encryption ...

Keywords: deep packet inspection, internet traffic identification, naive bayesian classification, measurement, pearson chi-square test

3 Revealing skype traffic: when randomness plays with you



Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, Paolo Tofanelli

October 2007 ACM SIGCOMM Computer Communication Review, Volume 37 Issue 4

Publisher: ACM

Full text available: Pdf (911.54 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 52, Downloads (12 Months): 745, Citation Count: 0

Skype is a very popular VoIP software which has recently attracted the attention of the research

community and network operators. Following a closed source and proprietary design, Skype protocols and algorithms are unknown. Moreover, strong encryption ...

Keywords: deep packet inspection, internet traffic identification, naive bayesian classification, measurement, pearson chi-square test

4 Certified email with a light on-line trusted third party: design and implementation



Martin Abadi, Neal Glew

May 2002 WWW '02: Proceedings of the 11th international conference on World Wide Web

Publisher: ACM

Full text available: Pdf (189.19 KB)

Additional Information: full citation, abstract, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 68, Citation Count: 11

This paper presents a new protocol for certified email. The protocol aims to combine security, scalability, easy implementation, and viable deployment. The protocol relies on a light on-line trusted third party that can be implemented without any special ...

5 Escrow services and incentives in peer-to-peer networks



Bill Horne, Benny Pinkas, Tomas Sander

October 2001 EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce

Publisher: ACM

Full text available: Pdf (265.69 KB)

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 53, Citation Count: 8

Distribution of content, such as music, remains one of the main drivers of P2P development. Scalable services are currently receiving a lot of attention from the content industry as a viable business model for P2P content distribution. One ...

6 TestU01: A C library for empirical testing of random number generators



Pierre L'Ecuyer, Richard Simard

August 2007 ACM Transactions on Mathematical Software (TOMS), Volume 33 Issue 4

Publisher: ACM

Full text available: Pdf (801.63 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 436, Citation Count: 1

We introduce *TestU01*, a software library implemented in the ANSI C language, and offering a set of utilities for the empirical statistical testing of uniform random number generators (RNGs). It provides general implementations of the classical ...

Keywords: Statistical software, random number generators, random number tests, statistical testing

7 Some facets of complexity theory and cryptography: A five-lecture tutorial



Jörg Rothe

December 2002 ACM Computing Surveys (CSUR), Volume 34 Issue 4

Publisher: ACM

Full text available: Pdf (2.78 MB)

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 50, Downloads (12 Months): 530, Citation Count: 1

In this tutorial, selected topics of cryptology and of computational complexity theory are presented give a brief overview of the history and the foundations of classical cryptography, and then move to modern public-key cryptography. Particular ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

8 High dynamic range imaging



Paul Debevec, Erik Reinhard, Greg Ward, Sumanta Pattanaik
August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes
Publisher: ACM

Full text available: Pdf (20.22 MB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 81, Downloads (12 Months): 790, Citation Count: 0

Current display devices can display only a limited range of contrast and colors, which is one of the reasons that most image acquisition, processing, and display techniques use no more than eight color channels. This course outlines recent ...

9 Compressed full-text indexes



Gonzalo Navarro, Veli Mäkinen
April 2007 ACM Computing Surveys (CSUR), Volume 39 Issue 1
Publisher: ACM

Full text available: Pdf (1.09 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 96, Downloads (12 Months): 960, Citation Count: 9

Full-text indexes provide fast substring search over large text collections. A serious problem of text indexes has traditionally been their space consumption. A recent trend is to develop indexes that exploit the compressibility of the text, so that ...

Keywords: Text indexing, entropy, text compression

10 Implementing sorting in database systems



Goetz Graefe
September 2006 ACM Computing Surveys (CSUR), Volume 38 Issue 3
Publisher: ACM

Full text available: Pdf (518.63 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 44, Downloads (12 Months): 1307, Citation Count: 2

Most commercial database systems do (or should) exploit many sorting techniques that are well known, but not readily available in the research literature. These techniques improve both sort performance on modern computer systems and the ability to ...

Keywords: Key normalization, asynchronous read-ahead, compression, dynamic memory resource allocation, forecasting, graceful degradation, index operations, key conditioning, nested iteration

11 Securing distributed storage: challenges, techniques, and systems



Vishal Kher, Yongdae Kim
November 2005 StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and systems
Publisher: ACM

Full text available:  Pdf (294.61 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 39, Downloads (12 Months): 384, Citation Count: 4

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy


12 [Charles W. Bachman interview: September 25-26, 2004; Tucson, Arizona](#)



Thomas Haigh

January 2006 ACM Oral History interviews

Publisher: ACM

Full text available:  Pdf (974.87 KB)

Additional Information: [full citation](#), [abstract](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 66, Downloads (12 Months): 511, Citation Count: 0

Charles W. Bachman reviews his career. Born during 1924 in Kansas, Bachman attended high school in East Lansing, Michigan before joining the Army Anti Aircraft Artillery Corp, with which he spent 1 year in the Southwest Pacific Theater, during ...

13 [Proceedings of the 2007 ACM symposium on Applied computing](#)



Yookun Cho, Yong Wan Koo, Roger L. Wainwright, Hisham M. Haddad, Sung Y. Shin

March 2007 proceeding

Publisher: ACM

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0



On behalf of the Organization Committee, it is our pleasure to welcome you to the 22nd Annual Symposium on Applied Computing (SAC 2007). This year, the conference is hosted by Seoul National University and Suwon University in Gyeonggi-do, Korea. ...

14 [Communications of the ACM: Volume 51 Issue 8](#)



August 2008 issue Volume 51 Issue 8

Publisher: ACM

Full text available:  Digital Edition ,  Pdf (6.85 MB) Additional Information: [full citation](#)



Bibliometrics: Downloads (6 Weeks): 3111, Downloads (12 Months): 3111, Citation Count: 0

15 [Communications of the ACM: Volume 51 Issue 9](#)



September 2008 issue Volume 51 Issue 9

Publisher: ACM

Full text available:  Digital Edition ,  Pdf (8.68 MB) Additional Information: [full citation](#)

Bibliometrics: Downloads (6 Weeks): 10345, Downloads (12 Months): 10345, Citation Count: 0



Facial modeling and animation

Jörg Haber, Demetri Terzopoulos

August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes

Publisher: ACM

Full text available: Pdf (18.15 MB)

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): 96, Downloads (12 Months): 954, Citation Count: 0

In this course we present an overview of the concepts and current techniques in facial modeling animation. We introduce this research area by its history and applications. As a necessary prere facial modeling, data acquisition is discussed ...



17 A survey of processors with explicit multithreading

Theo Ungerer, Borut Robič, Jurij Šilc

March 2003 ACM Computing Surveys (CSUR), Volume 35 Issue 1

Publisher: ACM

Full text available: Pdf (920.16 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index to](#)

Bibliometrics: Downloads (6 Weeks): 56, Downloads (12 Months): 544, Citation Count: 16

Hardware multithreading is becoming a generally applied technique in the next generation of microprocessors. Several multithreaded processors are announced by industry or already into p in the areas of high-performance microprocessors, media, ...

Keywords: Blocked multithreading, interleaved multithreading, simultaneous multithreading



18 ACM SIGACT News: Volume 36 Issue 4

December 2005 Issue Volume 36 Issue 4

Publisher: ACM

Additional Information: [full citation](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0



19 Total order broadcast and multicast algorithms: Taxonomy and survey

Xavier Défago, André Schiper, Péter Urbán

December 2004 ACM Computing Surveys (CSUR), Volume 36 Issue 4

Publisher: ACM

Full text available: Pdf (544.45 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index to](#)

Bibliometrics: Downloads (6 Weeks): 43, Downloads (12 Months): 499, Citation Count: 11

Total order broadcast and multicast (also called atomic broadcast/multicast) present an importa in distributed systems, especially with respect to fault-tolerance. In short, the primitive ensures messages sent to a set of processes are, ...

Keywords: Distributed systems, agreement problems, atomic broadcast, atomic multicast, clas distributed algorithms, fault-tolerance, global ordering, group communication, message passing taxonomy, total ordering



20 Real-time shading

Marc Olano, Kurt Akeley, John C. Hart, Wolfgang Heidrich, Michael McCool, Jason L. Mitchell, Randi

August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes



Publisher: ACM

Full text available: Pdf (7.39 MB)

Additional Information: full citation, abstract, cited by

Bibliometrics: Downloads (6 Weeks): 62, Downloads (12 Months): 727, Citation Count: 1

Real-time procedural shading was once seen as a distant dream. When the first version of this c offered four years ago, real-time shading was possible, but only with one-of-a-kind hardware or combining the effects of tens to hundreds of rendering ...

Results 1 - 20 of 786

Result page: 1 2 3 4 5 6 7 8 9 10 next >>

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 A

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: Adobe Acrobat QuickTime Windows Media Player RealPlayer